AO 91 (Rev. 11/11) Criminal Complaint (Rev. by USAO on 3/12/20) ☐ Original ☐ Duplicate Original

UNITED STATES DISTRICT COURT

for the

Central District of California

United States of America

v.

SAID RHAYEL,

Defendant

Case No. 2:23-mj-02500-DUTY

CRIMINAL COMPLAINT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, the complainant in this case, state that the following is true to the best of my knowledge and belief.

On or about the date of July 27, 2022 in the county of Los Angeles in the Central District of California, the defendant violated:

Code Section	*Offense Description*
18 U.S.C. § 1957	Transactional Money Laundering

This criminal complaint is based on these facts:

Please see attached affidavit.

☒ Continued on the attached sheet.

/S/ Jeremy Hess
Complainant's signature

Jeremy Hess, Special Agent IRS:CI
Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone.

Date: *May 16, 2023*

Judge's signature

City and state: Los Angeles, California

Hon. Alexander F. MacKinnon,
U.S. Magistrate Judge
Printed name and title

AUSA: James C. Hughes (#2579)

AFFIDAVIT

I, JEREMY HESS, being duly sworn, declare and state as follows:

I. INTRODUCTION

1. I am employed as a Special Agent with Internal Revenue Service, Criminal Investigation ("IRS:CI"). I have been employed in this capacity since September 2009. My responsibilities include the investigation of potential criminal violations of the Internal Revenue Code under Title 26 of the United States Code and offenses within Titles 18 and 31. I received formal training at the Federal Law Enforcement Training Center in conducting criminal investigations related to tax and other crimes. In my capacity as a Special Agent with IRS:CI, I have conducted investigations of a variety of tax and financial offenses and have executed search warrants resulting in the seizure of financial records and other evidence of criminal activity.

2. Since October 2021, I have been assigned to assist the U.S. Treasury Department Alcohol and Tobacco Tax and Trade Bureau ("TTB") with criminal investigations. Generally, TTB enforces the provisions related to tobacco manufacturing, importation, and operations under Title 26 of the United States Code. TTB works to enforce laws related to the federal excise tax of tobacco products and permitting required for the importation and manufacturing of these products.

3. Prior to my employment as a Special Agent, I was employed for seven years in the banking and financial services industry, most recently as a financial analyst. In addition to

my practical experience gained through employment, I obtained a Master of Business Administration degree from the University of South Florida in Tampa, Florida, as well as a Bachelor of Science degree in Business from Emporia State University in Emporia, Kansas.

II. PURPOSE OF AFFIDAVIT

1. This affidavit is made in support of a criminal complaint against, and arrest warrant for, SAID RHAYEL for a violation of 18 U.S.C. § 1957(a) (Transactional Money Laundering). This affidavit is also made in support of search warrants for the following premises more fully described in Attachment A-1, and two persons, as more fully described in Attachments A-2 and A-3:

a. 6233 Napoli Court, Long Beach, CA 90803 ("the SUBJECT PREMISES");

b. SAID RHAYEL ("RHAYEL"); and

c. MINYAN GUAN ("GUAN").

2. The requested search warrants seek authorization to seize evidence, fruits, or instrumentalities of violations of 18 U.S.C. § 545 (Smuggling); 18 U.S.C. § 1343 (Wire Fraud); 18 U.S.C. § 1956(a) and (h) (Money Laundering and Conspiracy to Commit Money Laundering); 18 U.S.C. § 1957 (Transactional Money Laundering); 26 U.S.C. 5762(a)(1) (Operating as a Tobacco Importer without a Permit); 26 U.S.C. 5762(a)(3) (Refusing or Attempting to Evade Federal Excise Taxes).

3. The facts set forth in this affidavit are based upon my personal observations, my training and experience, and

information obtained from various law enforcement personnel and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrants and does not purport to set forth all of my knowledge of or investigation into this matter. Unless specifically indicated otherwise, all conversations and statements described in this affidavit are related in substance and in part only.

III. SUMMARY OF PROBABLE CAUSE

4. IRS:CI, in coordination with U.S. Immigration and Customs Enforcement, Homeland Security Investigations ("HSI") is currently conducting an investigation into possible violations of the subject offenses by RHAYEL and others believed to be operating at RHAYEL's direction. Based on my review of various bank records, information and documentation provided by victims, and multiple witness interviews, I believe bank accounts under the control of RHAYEL and his associates, including GUAN, have received at least $3,000,000 in proceeds from various business email compromise frauds executed on victims across the country. Bank records obtained for accounts controlled by RHAYEL, GUAN, and others show that the abovementioned funds were rapidly disseminated amongst multiple accounts controlled by RHAYEL, GUAN, and others in a manner consistent with efforts to conceal and obfuscate the nature and source of the subject funds and prevent victims from locating and reclaiming their lost funds. Many of the accounts used by RHAYEL to receive and distribute funds are held in the name of business entities controlled by RHAYEL, GUAN, and their associates. Many of these same business

entities have also been linked to the illegal importation of untaxed foreign cigarettes through the Port of Los Angeles.

5. Based on statements provided by RHAYEL, and my own observations during interviews conducted during this investigation, I believe RHAYEL and GUAN both reside at the SUBJECT PREMISES. Based on my training and experience, and as described in further detail below, individuals involved in fraud schemes such as business email compromise frauds frequently retain and store information related to their fraudulent activities in their homes and on their digital devices. Accordingly, I find there is probable cause to believe that RHAYEL is engaged in the laundering of proceeds from criminal activities, including multiple instances of business email compromise fraud, as well as the illegal importation of untaxed foreign cigarettes, and that evidence of the abovementioned activities may be found at the SUBJECT PREMISES and on the persons of RHAYEL and GUAN.

6. In addition, based on my review of various bank records, information and documentation provided by victims, and multiple witness interviews, I believe RHAYEL has knowingly used funds derived from a business email compromise fraud, which fraud was perpetrated through the use of interstate wires, to complete a monetary transaction in or affecting interstate commerce, knowing that such funds constituted criminally derived property. Specifically, on or about July 27, 2022, RHAYEL wired $140,000, the vast majority of which constituted the proceeds of a business email compromise fraud, from a personal bank account

held by RHAYEL with Citibank, N.A., a federally insured bank, as part of the purchase price of a luxury foreign automobile.

IV. STATEMENT OF PROBABLE CAUSE

A. Business Email Compromise Fraud

7. Based on my training and experience, I know that a business email compromise scheme is a sophisticated financial fraud carried out through the malicious use of spoofed[1] email addresses designed to appear like those of legitimate vendors, customers, and business colleagues. Scammers will frequently use techniques such as spearphishing emails and malware to gain access to a victim's internal network, including email threads, and will use that access to impersonate business contacts and submit fraudulent requests for payment. The scammers will thereafter disperse the victim's funds amongst multiple subsidiary accounts to prevent the victim from recovering the funds by recalling the fraudulent payment.

B. RHAYEL, GUAN, and the SUBJECT PREMISES

8. Per California Secretary of State records and statements provided by RHAYEL, I know that RHAYEL is the owner and operator of multiple business entities purportedly engaged in the importation of various goods from overseas. GUAN is RHAYEL's spouse and the listed chief financial officer for Gray Light Logistics, Inc., a company ostensibly engaged in the importation of furniture. Both RHAYEL and GUAN reside in the

[1] Based on my training and experience, I know that the term "email spoofing" refers to the creation of email messages and accounts with forged sender addresses designed to appear like the accounts of trusted sources.

SUBJECT PREMISES, a single-family residence located in Long Beach, CA.

9. I first became aware of RHAYEL during a related investigation into multiple shipments of counterfeit goods and untaxed foreign cigarettes intercepted at Los Angeles International Airport and the Port of Los Angeles. Over the course of this related investigation, I have reviewed customs documentation for the abovementioned seizures, as well as memorandums describing multiple surveillance operations conducted by IRS:CI with the assistance of TTB investigators. I have also conducted multiple witness interviews, including interviews of RHAYEL, his associate, Jun Liu, and others. Based on my review of the abovementioned information and documentation, I state as follows:

10. On or about November 9, 2021, Customs and Border Protection ("CBP") officers at Los Angeles International Airport intercepted a shipment of goods from China containing approximately 786 cartons of foreign cigarettes concealed inside hollow boxes designed to appear like ottomans. The shipment was falsely manifested as "computer chairs," with no federal excise taxes reflected on customs entry documents, and was consigned to Guangzho Whale Trading, CO LTD., with a listed address at 24300 Nandina Avenue, Moreno Valley, CA 92551, an Amazon fulfillment center.

11. On or about December 13, 2021, the abovementioned shipment of foreign cigarettes was released from CBP custody in order to permit investigating agents to follow the shipment to

its ultimate destination. After the shipment was retrieved by a third-party trucking company, IRS:CI Special Agent Joshua Culbertson, with assistance from TTB investigators, followed the shipment to a warehouse facility controlled by Jun Liu located at 956 W. 10th Street, Azuza, California.

12. Between April 2022 and October 2022, CBP officers at the Port of Los Angeles intercepted multiple shipments of falsely manifested goods from China containing foreign cigarettes concealed in metal boxes designed to appear like electronic medical devices. At least five of these shipments were subsequently linked to Jun Liu based on customs paperwork filed in relation to the shipments listing Jun Liu's employees and associates as points of contact. One of the shipments linked to Jun Liu containing concealed foreign cigarettes was a shipment intercepted on or about September 14, 2022, consigned to Triple Five International, Inc. ("Triple Five"). California Secretary of State documents for Triple Five show that the company was incorporated on March 8, 2022, with a listed address at 956 W. 10th Street, Azusa, California, and with Fion Liu as the company's agent for service of process. Based on an interview I conducted with Jun Liu on November 30, 2022, I know that Fion Liu is Jun Liu's daughter.

13. On or about January 18, 2023, I conducted an interview of RHAYEL in the garage of his residence at the SUBJECT PREMISES. During the interview, RHAYEL made the following representations:

a. RHAYEL acknowledged that he was the owner and operator of the businesses Junyu International Supply Chain (USA) Inc. ("Junyu") and Nanokeratin Technologies ("Nanokeratin"), and that he had previously operated JC Auto Rental ("JC Auto") with another individual. RHAYEL claimed that he had opened Nanokeratin to import hair care products and Junyu to import picture frames. However, RHAYEL also acknowledged that he had used both Nanokeratin and Junyu to import cargo on behalf of an individual in China whom he knew as "Mr. Chen."

b. RHAYEL admitted that he had assisted Jun Liu and Fion Liu with the importation of cargo on behalf of Mr. Chen and claimed that Jun Liu and Fion Liu had previously hired him to import containers, clear customs, and truck containers to Jun Liu's warehouse. RHAYEL stated that he helped to import three containers for Triple Five, but that he had stopped assisting with shipments for this company after a shipment was seized by CBP following the execution of a search warrant.

c. In addition to his own business entities, RHAYEL also claimed to assist his wife, GUAN, with her furniture import business, Gray Light Logistics. RHAYEL stated that he handled everything related to Gray Light Logistics because GUAN did not "speak English."

d. RHAYEL identified Kayvan Kesla ("Kesla") as an individual who performed trucking services for RHAYEL's business entities and stated that Kesla was the owner of The Lawgistics Group ("Lawgistics Group"). RHAYEL stated that Kesla only provided trucking services for RHAYEL, and that Kesla never

actually imported goods into the United States on his own behalf.

e. RHAYEL acknowledged that all of his business entities were operated out of a warehouse that he maintains at 4427 Rowland Avenue in El Monte, California.

C. Business Email Compromise Proceeds Linked to RHAYEL and GUAN

14. Based on my review of bank records for business entities owned or controlled by RHAYEL, and information and documentation provided by representatives of various victim businesses, I have identified multiple occasions in which bank accounts controlled by RHAYEL received, and subsequently disbursed, funds traceable to business email compromise frauds perpetrated against victims throughout the country. Information regarding RHAYEL's receipt of these fraudulently obtained funds is provided below.

1. Opler Flooring - $65,000

15. Opler Flooring ("Opler") is a commercial and residential flooring contractor based in Miami, Florida. On February 3, 2023, I conducted an interview of Opler's owner Lalitkumar Gadwani ("Gadwani"). Based on my conversation with Gadwani and my review of the police report filed by Opler on January 16, 2020, I state as follows:

a. On or around January 3, 2020, representatives of Opler received an email from a spoofed email address designed to mimic the account of one of Opler's vendors. The email requested that Opler remit payment on a recently completed

purchase in accordance with wiring instructions attached to the email. The attached wiring instructions listed an account held in the name of Junyu International Supply Chain Company with JP Morgan Chase Bank ("JPMC") with the account number ending #2790 ("Junyu JPMC Account").

b. On or around January 14, 2020, Opler wire transferred $65,000 to the Junyu JPMC Account in accordance with the instructions received from the spoofed email address. When representatives of Opler subsequently contacted their vendor to request the release of Opler's order, they were informed that the vendor had never received payment. After reviewing their emails, representatives of Opler determined that the company was the victim of an "email phishing scam."

16. I have reviewed bank records for the Junyu JPMC Account. The signature card for the account lists RHAYEL as sole signatory. Account statements and deposit/withdrawal records for the account show the following transactions:

a. On January 14, 2020, the Junyu JPMC Account received a $65,000 wire transfer from Opler.

b. On January 15, 2020, $10,500 was withdrawn from the Junyu JPMC Account via a $5,500 cash withdrawal and the purchase of a $5,000 cashier's check in the name of GUAN. On the same date, $13,952 was wired from the Junyu JPMC Account to an account held in the name of Yutong Guan with Bank of America, and $10,000 was wired to an account held in the name of Mohammed Rhayel with Toronto Dominion Bank.

c. On January 16, 2020, $6,000 in cash was withdrawn from the Junyu JPMC Account. The Junyu JPMC Account was subsequently frozen following JPMC's discovery of the subject fraud.

17. On January 17, 2020, RHAYEL spoke with JPMC fraud group manager Brian Stephenson ("Stephenson") on the telephone and questioned why his account had been frozen. I have spoken with Stephenson regarding his conversation with RHAYEL. Per Stephenson, RHAYEL informed him that the fraudulent transfer into his account was from a "longtime customer" named "Balil" who operated a logistics company. RHAYEL told Stephenson that he would call him back with additional information but made no further contact with Stephenson thereafter.

2. Sunridge Management Corporation - $107,065.91

18. Sunridge Management Corporation ("Sunridge") is a property management business located in Dallas, Texas. On February 6, 2023, I conducted an interview of Sunridge's Information Technology Manager James Bradley ("Bradley"). Based on my conversation with Bradley, my review of the written statement provided by Sunridge employee, Karen Smith ("Smith"), to JPMC on June 16, 2021, and my review of supporting emails and documentation provided by Sunridge to JPMC pursuant to the company's fraud referral, I state as follows:

a. On June 9, 2021, Smith received an email from an individual who Smith believed to be a representative of the owner of one of the properties managed by Sunridge. In the email, the alleged owner representative provided Sunridge with

wiring instructions for a payment the owner allegedly wished to be made from the property operating account managed by Sunridge. In fact, the email received by Smith on June 9, 2021, was issued from a spoofed email address designed to mimic the account of the subject owner representative.

b. On June 9, 2021, believing the abovementioned email to be legitimate, Smith instructed Sunridge's staff accountant to execute the requested wire transfer. Sunridge subsequently transferred $107,065.91 to an account held in the name of Nanokeratin Technologies with JPMC with the account number ending #7669 ("the Nanokeratin JPMC Account").

19. I have reviewed bank records for the Nanokeratin JPMC Account as well as other accounts that received transfers of funds from this account. Based on my review of these records, I state as follows:

a. RHAYEL is the sole signatory on the Nanokeratin JPMC Account.

b. On June 9, 2021, the Nanokeratin JPMC Account received an intrabank transfer of $107,065.91 from Sunridge. Immediately after this transfer was received, $107,065,91 was transferred from the Nanokeratin JPMC Account to an account held with JPMC in the name of JC Auto Rental with the account number ending #1125 ("the JC Auto JPMC Account"). RHAYEL is the sole signatory on the JC Auto JPMC Account.

c. On June 10, 2021, $100,000 was wired from the JC Auto JPMC Account to an account held with East West Bank in the

name of GUAN with the account number ending #5871 ("the Guan EWB Account").

3. American Agroproducts Inc. - $104,982.73

20. American Agroproducts, Inc. ("AAI") is a flower wholesaling business based in Dallas, Texas. On February 16, 2023, I conducted an interview of AAI employee Diana Massey ("Massey"). During the interview, Massey informed me that AAI had previously been the victim of a business email compromise scheme. In March 2022, AAI issued multiple wire transfers in response to payment requests received from a spoofed email address designed to mimic the email account of an employee of one of AAI's vendors. The emails received from the spoofed email address directed AAI to make payments to an account held with JPMC with the account number ending #6231. After issuing the abovementioned payments, AAI employees learned that the spoofed email address was fake, and that AAI's vendor had never received the issued payments.

21. Bank records for the JPMC bank account with the account number ending #6231 show that the account is held in the name of Kayvan Kesla and was opened in February 2022 ("the Kesla JPMC Account"). Based on my review of bank records for the Kesla JPMC Account and other accounts that received funds from this account, I state as follows:

a. Between March 18, 2022 and March 21, 2022, AAI transferred $104,982.73 to the Kesla JPMC Account via three wire transfers.

b. Between March 14, 2022 and March 30 2022, the Kesla JPMC account received four wire transfers, together totaling approximately $187,251, from foreign bank accounts held in the name of Positronica S.A. ("Positronica"). Positronica's website indicates the company is a medical device wholesaler located in the Canary Islands. Given the size of the wire transfers, the absence of any discernible connection between Kesla and Positronica, and the ultimate disposition of the funds (described below), I believe the funds received by the Kesla JPMC Account from Positronica likely constitute the proceeds of some fraudulent activity.

c. Prior to its receipt of the wire transfers from AAI and Positronica, together totaling approximately $292,234, the Kesla JPMC Account had a balance of only $5.00.

d. On or about March 17, 2022, $12,150 was wire transferred from the Kesla JPMC Account to an account held with Citibank in the name of Junyu International Supply Chain Company (USA), Inc., with the account number ending #6897 ("the Junyu Citibank Account"). Two additional wire transfers were subsequently sent to the Junyu Citibank Account on March 21, 2022 ($50,000) and March 22, 2022 ($189,685) respectively.

e. Bank records for the Junyu Citibank Account show that the sole signatory on the account is RHAYEL.

f. On or about March 23, 2022, $25,000 was wired from the Junyu Citibank Account to an account held in the name of Aloha Sportfishing ("Aloha"), a sport fishing boat charter service. Based on my review of bank records for other accounts

controlled by RHAYEL, and my review of public vehicle registration records, I believe the $25,000 transfer to Aloha reflected a portion of the purchase price of a motorboat purchased by RHAYEL from Aloha.

g. On or about March 23, 2022, $72,500 was wired from the Junyu Citibank Account to an account held in the name of Xinghung International, Inc. with U.S. Bank, NA ("the Xinghung U.S. Bank Account"). On March 29, 2022, an additional $30,000 wire was issued from the Junyu Citibank Account to the Xinghung U.S. Bank Account.

4. C&G Farms, Inc. - $800,729.53

22. C&G Farms, Inc. ("C&G") is a family run farming operation in Ripon, California. On February 14, 2023, I conducted an interview of C&G Farms employee Michael Amaral ("Amaral"). Based on my conversation with Amaral, my review of the referral submitted by C&G to the Federal Bureau of Investigation on August 4, 2022, and my review of various items of email correspondence provided by C&G, I state as follows:

a. On July 13, 2022, multiple C&G employees, including Amaral, received an email from an individual who they believed to be a representative of one of C&G's vendors. In fact, the email was sent from a spoofed email address designed to mimic the email domain of C&G's vendor. In the email, the purported vendor representative instructed the C&G employees that all future payments to the vendor would need to be made through ACH transfer to an account held with Citibank with the account number ending #0493.

b. On July 18, 2022, the same spoofed email address sent the C&G employees a follow-up email stating that the bank account information provided in the previous email was incorrect, and that C&G should instead send future payments via ACH transfer to an account held with Citibank with the account number ending #5558.

c. On or about July 20, 2022, believing the abovementioned emails to be legitimate, C&G employees transferred approximately $800,729.53 to the Citibank account with the account number ending #5558.

23. Bank records for the Citibank account with the account number ending #5558 show that the account is held in the name of Nanokeratin Technologies Inc. ("the Nanokeratin Citibank Account") and that RHAYEL is the sole signatory. Based on my review of bank records for the Nanokeratin Citibank Account and other accounts that received funds from this account I state as follows:

a. On or about July 20, 2022, the Nanokeratin Citibank Account received an ACH transfer from C&G in the amount of $800,729.53. Prior to the abovementioned transfer, the Nanokeratin Citibank Account had a $5,000 balance.

b. On or about July 21, 2022, RHAYEL withdrew $255,000 from the Nanokeratin Citibank Account via the purchase of a $15,000 cashier's check payable to GUAN, a $50,000 intrabank transfer to Junyu International Supply Chain, and a $190,000 intrabank transfer to an account held by RHAYEL with Citibank in his own name with the account number ending #8852

("the Rhayel Citibank Account"). RHAYEL subsequently wired $140,000 from the Rhayel Citibank Account on July 25, 2022, as part of the purchase price of a new automobile.

c. On or about July 25, 2022, RHAYEL withdrew $235,000 from the Nanokeratin Citibank Account via a $200,000 intrabank transfer to the Junyu Citibank Account and the purchase of a $35,000 cashier's check payable to himself.

d. Between July 27, 2022, and August 4, 2022, four wire transfers, together totaling $170,000, were sent from the Junyu Citibank Account to an account held with Zhejiang Tailong Commercial Bank in the name of Fenda Trading Company Limited.

5. Muse Railroad Materials, LLC - $1,969,000

24. Muse Railroad Materials, LLC ("Muse") is a corporation specializing in railroad material purchasing and sales with its principal place of business in Buford, Georgia. On January 5, 2023, I conducted an interview of Muse employee, Derrick Kilgore. Based on my conversation with Kilgore, my review of various items of email correspondence provided by Muse, and my review of bank records for accounts controlled by Muse, I state as follows:

a. In September 2022, Muse submitted a bid for the purchase of a large volume of scrap rail from Norfolk Southern Corporation ("Norfolk Southern"), a railroad operator, for $1,969,000. Muse's bid was subsequently accepted by Norfolk Southern.

b. On October 17, 2022, Derrick Kilgore received an email from an individual whom he believed to be an employee of

Norfolk Southern. The email instructed Muse to remit payment on its bid, via wire transfer, to an account held with Citibank with the account number ending #4483. In fact, the abovementioned email was sent via a spoofed email address designed to mimic the email address of a Norfolk Southern employee.

c. On or about October 17, 2022, believing the abovementioned email to be legitimate, Muse employees wire transferred $1,969,000 to the Citibank account with the account number ending #4483.

25. Bank records obtained from Citibank show that bank account #4483 is held in the name of Triple Five International, Inc., and that the sole signatory on the account is Fion Liu ("the Triple Five Citibank Account"). Based on my review of bank records for the Triple Five Citibank Account and other accounts that received funds from this account I state as follows:

a. On or about October 17, 2022, the Triple Five Citibank Account received a $1,969,000 wire transfer from Muse's bank account.

b. On October 20, 2022, Triple Five, Inc. wire transferred $569,000 to an account held with Bank of America in the name of Inland Empire Materials, LLC ("Inland Empire Materials") with the account number ending #9226 ("the Inland Empire BOA Account"). The Inland Empire BOA Account had previously been opened by Amanda Atef Al-Said ("Al-Said") on October 12, 2022, and had a zero balance at the time of the deposit of funds from the Triple Five Citibank Account.

According to my analysis of bank records, Al-Said lives with and is married to Kesla. Based on my investigation, I have learned that Al-Said has made bank transactions referring to Kesla as her husband.

c. On October 21, 2022, Triple Five executed a wire transfer in the amount of $431,000 to an account held in the name of EM Trading, LLC ("EM Trading") with Bank of America with the account number ending #8286 ("the EM Trading BOA Account"). The signatories on the EM Trading Account are Deandre Raymond Pool ("Pool") and Henry Lee Meza ("Meza"). Based on my review of bank records for accounts controlled by RHAYEL, and statements made by RHAYEL during his interview, I believe Henry Lee Meza and Deandre Raymond Pool are warehouse workers employed by RHAYEL. During his interview, RHAYEL mentioned Meza was his employee. Further, I have seen Pool's name as a payee on multiple checks from RHAYEL, consistent with the amount that RHAYEL pays his other employees.

d. On October 24, 2022, Inland Empire Materials wire transferred $50,000 to an account held with U.S. Bank in the name of Junyu International Supply Chain (USA) Inc. with the account number ending #1393 ("the Junyu U.S. Bank Account"), and $160,000 to an account held with JPMC in the name of Gray Light Logistics with the account number ending #1965 ("the Gray Light JPMC Account"). Subsequently, between October 25, 2022, and October 31, 2022, Inland Empire Materials transferred an additional $400,000 to the Junyu U.S. Bank Account via four wire transfers of $100,000. Bank records for the abovementioned

accounts show that RHAYEL is the sole signatory on the Junyu U.S Bank Account and GUAN is the sole signatory on the Gray Light JPMC Account.

e. On October 24, 2022, EM Trading wire transferred $180,000 to the Junyu U.S. Bank Account, $120,000 to the Gray Light JPMC Account, and $40,000 to an account held in the name of Global Star Trading, Inc. with JPMC ("the Global Star JPMC Account"). Subsequently, on January 18, 2023, $40,000 was wired from the Global Star JPMC Account to an account held in the name of Junyu International Supply Chain Company (USA), Inc. with Bank of the West with the account number ending #7242 ("the Junyu BOW Account"). Bank records for the Junyu BOW Account show that RHAYEL is the sole signatory on the account.

f. On October 24, 2022, a cashier's check in the amount of $65,000 was purchased from the EM Trading BOA Account. The cashier's check was subsequently deposited into an account held with U.S. Bank in the name of RHAYEL with the account number ending #1401 ("the Rhayel U.S. Bank Account"). Bank records for the Rhayel U.S. Bank Account show that RHAYEL is the sole signatory.

g. On October 25, 2022, $3,500 was sent from Inland Empire BOA Account to the Rhayel U.S. Bank Account via the Zelle Peer-to-Peer digital payment application. An additional $3,000 Zelle transfer from the EM Trading BOA Account was subsequently issued to the Rhayel U.S. Bank Account on October 26, 2022.

h. On October 28, 2022, EM Trading wire transferred an additional $169,000 to the Junyu U.S. Bank Account.

i. On November 7, 2022, $100,000 was wire transferred from the Gray Light JPMC Account to an account held in the name of Yiwu Lucky Rare Trading Co. Ltd. with Zhejiang Tailong Commercial Bank.

j. Between November 9, 2022 and November 17, 2022, wire transfers were issued from the Junyu U.S. Bank Account to the following parties:

i. Zhejiang Doyin Technology Company Ltd. ($70,000);

ii. Mabmedia LLC ($50,000);

iii. Shandong Ruicheng Weaving Co. Ltd. ($50,000);

iv. Yiwu Lucky Rare Trading Co. Ltd. ($70,000); and

v. Miami Games Distributor ($50,000).

k. On November 22, 2022, $106,415.61 was withdrawn from the Junyu U.S. Bank Account via the purchase of a cashier's check payable to Mercedes Benz of Arcadia, an auto dealership located in Arcadia, California. Based on my review of California vehicle registration records, I believe that the abovementioned check was used as part of the purchase price of an automobile bought by RHAYEL.

l. On November 28, 2022, $84,000 was withdrawn from the Junyu U.S. Bank Account via the purchase of a cashier's check payable to RHAYEL with the notation "SALARY." The check was subsequently deposited into an account held in the name of

RHAYEL with Bank of the West with the account number ending #6939 ("the Rhayel BOW Account").

m. On November 29, 2022, $290,000 was withdrawn from the Junyu U.S. Bank Account via the purchase of a cashier's check payable to Junyu International Supply Chain (USA) Inc. The cashier's check was subsequently deposited into the Junyu BOW Account.

D. Cigarette Seizures Linked to Rhayel Associated Entities

26. Based on my review of CBP seizure records, I have identified multiple occasions in which entities owned and/or controlled by RHAYEL were linked to shipments of goods intercepted at the Port of Los Angeles containing concealed foreign cigarettes. Information regarding these shipments is provided below.

a. On June 29, 2022, pursuant to border search authority, CBP officers conducted a search of a container shipment of goods with the bill of lading number MATS-1510019000, which had arrived at the Port of Los Angeles from China. Customs paperwork filed for the abovementioned shipment, including customs entry documents and packing lists, listed the imported goods as "picture frames" and reported no taxes due and owing on the imported goods. Upon searching the abovementioned shipment, CBP officers discovered multiple packages containing unmanifested metal boxes labeled "Electric Welding Machine" and "Voltage Regulator." Upon opening the metal boxes, CBP officers discovered bundles of foreign brand cigarettes concealed within

each box. In total, CBP officers seized approximately 2,343 cartons of unmanifested foreign cigarettes on which no federal excise taxes were reported or paid. CBP officers also discovered multiple boxes containing counterfeit luxury goods including fake Louis Vuitton and Gucci handbags and Nike shoes. Customs entry documents and packing lists for the abovementioned shipment list the importer of record as Lawgistics Group, 4427 Rowland Avenue, El Monte CA.

b. On July 27, 2022, pursuant to border search authority, CBP officers conducted a search of a container shipment of goods with the bill of lading number ZIMU-SHH30864123, which had arrived at the Port of Los Angeles from China. Customs paperwork filed for the abovementioned shipment, including customs entry documents and packing lists, listed the imported goods as "picture frames" and reported no taxes due and owing on the imported goods. Upon searching the abovementioned shipment, CBP officers discovered multiple packages containing unmanifested metal boxes labeled "Electric Welding Machine" and "Voltage Regulator." Upon opening the metal boxes, CBP officers discovered multiple bundles of foreign brand cigarettes concealed within. In total, CBP officers seized approximately 2,688 cartons of unmanifested foreign cigarettes on which no federal excise taxes were reported or paid. CBP officers also discovered multiple boxes containing counterfeit luxury goods including fake Louis Vuitton and Gucci handbags and Adidas shoes. Customs entry documents and packing lists for the abovementioned shipment list the importer of record as Junyu

International Supply Chain (USA) Inc., 4427 Rowland Avenue, El Monte CA.

c. On August 5, 2022, pursuant to border search authority, CBP officers with the CBP Merchandise Enforcement Team conducted a search of a container shipment of goods, container number #MATU4587972, which had arrived at the Port of Los Angeles from China. Customs paperwork filed for the abovementioned shipment, including customs entry documents and shipping manifests, listed the imported goods as "picture frames" and reported no taxes due and owing on the imported goods. Upon searching the abovementioned shipment, CBP officers discovered multiple packages containing unmanifested metal boxes that appeared to be electronic devices. Upon opening the metal boxes, CBP officers discovered multiple bundles of foreign brand cigarettes. In total, CBP officers seized approximately 1,960 cartons of unmanifested foreign cigarettes on which no federal excise taxes were reported or paid. Customs entry documents and shipping manifests for the abovementioned shipment list the importer of record as Nanokeratin Technologies, Inc., 4427 Rowland Avenue, El Monte CA.

E. Specific Evidence of Transactional Money Laundering

27. As previously described in paragraph 22(a) above, on or about July 20, 2022, $800,729.53 was ACH transferred by C&G Farms into a Citibank checking account controlled by RHAYEL and held in the name of Nanokeratin Technologies ("the C&G Farms ACH Transfer"). Based on my review of bank records for the Nanokeratin Citibank Account, my review of the referral

submitted by C&G Farms to the Federal Bureau of Investigation on August 4, 2022, and my review of various items of email correspondence provided by C&G Farms to the government as part of this investigation, I believe C&G Farms wired the abovementioned funds to the Nanokeratin Citibank Account as the result of a business email compromise scheme perpetrated against C&G Farms. Additional information regarding this fraud was previously provided in paragraphs 21 and 22 above.

28. The C&G Farms ACH Transfer was transmitted via the Federal Reserve Banks' automated clearing house service ("FedACH"), an electronic fund transfer system providing inter-bank clearing of credit and debit transactions. Based on information provided by the Federal Reserve Bank of Atlanta, I know that FedACH payments are processed over a network that connects all twelve Federal Reserve Banks, and that payment transactions processed through the network are routed through a processing site located in New Jersey. Accordingly, based on my review of documentation provided by C&G Farms, bank records for the Nanokeratin Citibank Account, and records and documentation provided by the Federal Reserve Bank of Atlanta, I believe the business email compromise fraud perpetrated against C&G Farms involved the use of interstate wires.

29. As previously described in paragraph 22(b), on or about July 21, 2022, RHAYEL transferred $190,000 from the Nanokeratin Citibank Account to the RHAYEL Citibank Account. Based on my review of bank records for the Nanokertain Citibank Account, I know that the transferred funds were derived from the

C&G Farms ACH Transfer. Prior to the C&G Farms ACH transfer on July 20, 2022, the Nanokeratin Citibank Account had a $5,000 balance. Additionally, between July 20, 2022 and July 21, 2022, no other deposits were made into the Nanokeratin Citibank Account. Accordingly, the C&G Farms ACH Transfer was the sole source of funds used in the $190,000 transfer from the Nanokeratin Citibank Account to the RHAYEL Citibank Account.

30. Bank records for the RHAYEL Citibank Account show that on July 27, 2022, $140,000 was wired from the RHAYEL Citibank Account to an account held with Wells Fargo Bank in the name of JLR Puente Hills, LLC ("the JLR Wire Transfer"). Based on my review of bank records for the Rhayel Citibank Account, I know that the funds used in the JLR Wire Transfer were predominantly derived from the earlier $190,000 transfer received from the Nanokeratin Citibank Account. Prior to the $190,000 transfer from the Nanokeratin Citibank Account, the RHAYEL Citibank Account had a balance of only $1,738.29. Additionally, between July 21, 2022 and July 25, 2022, the only other deposit into the RHAYEL Citibank Account was a $2,729.53 deposit executed on July 25, 2022. Accordingly, funds transferred from the Nanokeratin Citibank Account represented the vast majority of the funds used in the JLR Wire Transfer.

31. Based on my training and experience, and the information accumulated over this investigation, I believe RHAYEL's banking transactions following his receipt of the C&G Farms ACH Transfer, which transactions are summarized in paragraphs 23, 29, and 30 above, reflect a deliberate effort to

rapidly disseminate the subject funds in order to place them beyond the easy reach of the victim, C&G Farms. I believe RHAYEL's behavior evidences that he is aware that the subject funds constitute the proceeds of criminal activities that are potentially subject to seizure by the financial institutions used to receive and transmit the funds.

32. Purchase records provided by Jaguar Land Rover Puente Hills, an automotive dealership located in City of Industry, California ("JLR PH") show that the JLR Wire Transfer was used by RHAYEL as part of the purchase price of a new automobile. On July 27, 2022, RHAYEL purchased a 2022 Land Rover, Range Rover Sport SVR, from JLR PH for a total sales price, including fees and taxes, of $157,832 ("the Range Rover Purchase"). The JLR Wire Transfer provided the majority of the funds used by RHAYEL to complete this purchase.

33. Based on my training and experience and my review of the BankFind Suite database maintained by the Federal Deposit Insurance Corporation, I know that Citibank is a federally insured bank.

34. Based on my training and experience, and my review of publicly available information regarding Land Rover vehicles, I know that these vehicles are luxury automobiles manufactured outside of the United States. Accordingly, the purchase and sale of these automobiles necessarily affects interstate commerce.

35. Based on the abovementioned information, I believe there is probable cause to find that the Range Rover Purchase

was, in fact, a monetary transaction derived from the proceeds of wire fraud within the meaning of 18 U.S.C. § 1343, and that RHAYEL knowingly engaged in the Range Rover Purchase knowing that the transaction involved criminally derived property.

V. TRAINING AND EXPERIENCE ON FRAUD SCHEMES

36. Based on my training and experience, and the nature of the fraudulent scheme currently under investigation, I submit that there is probable cause to believe that evidence of the Subject Offenses will be found at the residence of RHAYEL and GUAN, and on their persons. Typically, individuals involved in fraud schemes maintain evidence where it is close at hand and safe, such as in their residences, vehicles, and digital devices, which are also commonly stored in their residences and vehicles.

37. Individuals involved in complex financial frauds, including business email compromise schemes, frequently send emails and/or text messages related to their schemes to defraud, which communications require the use of digital devices. I know that individuals who commit crimes with the aid of electronic devices do not readily discard them, because computers, tablets, and cell phones are expensive items that are typically used for years before being upgraded or discarded. Computers, tablets, and cell phones can also be used to communicate between co-conspirators and may contain information relating to the crime under investigation. Additionally, even when individuals who use digital devices to commit fraud upgrade their devices, they

often transfer data across devices, such as contact lists, email and text communications, and documentary records.

38. Individuals involved in fraud frequently keep the most damaging evidence and/or proceeds of the scheme at their residences and in their vehicles to help conceal the fraud from third parties, such as coworkers or employees, who may have access to such documents at the workplace. Proceeds such as cash and gifts are easier to conceal at the fraudster's residence rather than in plain view at a place of business.

39. Individuals involved in fraud and money laundering frequently use fraudulent proceeds to purchase cryptocurrency as a means of concealing and obscuring the source and location of the subject funds.[2] In addition, individuals involved in money laundering conspiracies frequently employ cryptocurrency as a means of transmitting funds between and amongst co-conspirators due to the anonymity afforded by a cryptocurrency wallet[3] versus a traditional bank account. Individuals involved in fraud and money laundering who purchase cryptocurrency will typically maintain their cryptocurrency wallets in a safe and secure location, such as their homes, to prevent the theft or destruction of the wallet. In addition, many individuals involved in the purchase and sale of cryptocurrency, in general,

---

[2] To date, I have not identified any specific transactions in my investigation evidencing RHAYEL or GUAN's purchase of cryptocurrency using the proceeds of business email compromise schemes.

[3] Based on my training and experience, I know that a cryptocurrency "wallet" is a device, software program, or a service which stores and maintains the public and/or private keys for cryptocurrency transactions.

maintain cryptocurrency wallets accessible on their digital devices such as smart phones and tablets, which devices are typically stored in the home or on the person of the device owner.

40. More sophisticated criminals may rent public storage units, safe deposit boxes, or other third-party space to further distance themselves from incriminating evidence or to hide their illicit profits from law enforcement or civil litigants. Such individuals typically maintain items relating to those third-party locations at their homes, such as keys, addresses, and leasing documents.

41. The requested search warrant seeks not only to seize evidence of crimes but also the "fruits of crime" and "property designed for use, intended for use, or used in committing a crime." Fed. R. Crim. P. 41(c). Even long after a crime has been completed, the illicit proceeds of a crime often still exist, frequently secreted in forms or locations difficult to detect by law enforcement.

VI. TRAINING AND EXPERIENCE ON DIGITAL DEVICES[4]

42. Based on my training, experience, and information from those involved in the forensic examination of digital devices, I

[4] As used herein, the term "digital device" includes any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop, laptop, notebook, and tablet computers; personal digital assistants; wireless communication devices, such as paging devices, mobile telephones, and smart phones; digital cameras; gaming consoles; peripheral input/output devices, such as keyboards, printers, scanners, monitors, and drives; related communications devices, such as modems, routers, cables, and connections; storage media; and security devices.

know that the following electronic evidence, inter alia, is often retrievable from digital devices:

a. Forensic methods may uncover electronic files or remnants of such files months or even years after the files have been downloaded, deleted, or viewed via the Internet. Normally, when a person deletes a file on a computer, the data contained in the file does not disappear; rather, the data remain on the hard drive until overwritten by new data, which may only occur after a long period of time. Similarly, files viewed on the Internet are often automatically downloaded into a temporary directory or cache that are only overwritten as they are replaced with more recently downloaded or viewed content and may also be recoverable months or years later.

b. Digital devices often contain electronic evidence related to a crime, the device's user, or the existence of evidence in other locations, such as, how the device has been used, what it has been used for, who has used it, and who has been responsible for creating or maintaining records, documents, programs, applications, and materials on the device. That evidence is often stored in logs and other artifacts that are not kept in places where the user stores files, and in places where the user may be unaware of them. For example, recoverable data can include evidence of deleted or edited files; recently used tasks and processes; online nicknames and passwords in the form of configuration data stored by browser, e-mail, and chat programs; attachment of other devices; times the device was in use; and file creation dates and sequence.

c. The absence of data on a digital device may be evidence of how the device was used, what it was used for, and who used it. For example, showing the absence of certain software on a device may be necessary to rebut a claim that the device was being controlled remotely by such software.

d. Digital device users can also attempt to conceal data by using encryption, steganography, or by using misleading filenames and extensions. Digital devices may also contain "booby traps" that destroy or alter data if certain procedures are not scrupulously followed. Law enforcement continuously develops and acquires new methods of decryption, even for devices or data that cannot currently be decrypted.

43. Based on my training, experience, and information from those involved in the forensic examination of digital devices, I know that it is not always possible to search devices for data during a search of the premises for a number of reasons, including the following:

a. Digital data are particularly vulnerable to inadvertent or intentional modification or destruction. Thus, often a controlled environment with specially trained personnel may be necessary to maintain the integrity of and to conduct a complete and accurate analysis of data on digital devices, which may take substantial time, particularly as to the categories of electronic evidence referenced above. Also, there are now so many types of digital devices and programs that it is difficult to bring to a search site all of the specialized manuals, equipment, and personnel that may be required.

b. Digital devices capable of storing multiple gigabytes are now commonplace. As an example of the amount of data this equates to, one gigabyte can store close to 19,000 average file size (300kb) Word documents, or 614 photos with an average size of 1.5MB.

44. The search warrant requests authorization to use the biometric unlock features of a device, based on the following, which I know from my training, experience, and review of publicly available materials:

a. Users may enable a biometric unlock function on some digital devices. To use this function, a user generally displays a physical feature, such as a fingerprint, face, or eye, and the device will automatically unlock if that physical feature matches one the user has stored on the device. To unlock a device enabled with a fingerprint unlock function, a user places one or more of the user's fingers on a device's fingerprint scanner for approximately one second. To unlock a device enabled with a facial, retina, or iris recognition function, the user holds the device in front of the user's face with the user's eyes open for approximately one second.

b. In some circumstances, a biometric unlock function will not unlock a device even if enabled, such as when a device has been restarted or inactive, has not been unlocked for a certain period of time (often 48 hours or less), or after a certain number of unsuccessful unlock attempts. Thus, the opportunity to use a biometric unlock function even on an

enabled device may exist for only a short time. I do not know the passcodes of the devices likely to be found in the search.

c. Thus, the warrant I am applying for would permit law enforcement personnel to, with respect to any device that appears to have a biometric sensor and falls within the scope of the warrant: (1) depress RHAYEL's and/or GUAN's thumb and/or fingers on the device(s); and (2) hold the device(s) in front of RHAYEL's and/or GUAN's face with his or her eyes open to activate the facial-, iris-, and/or retina-recognition feature.

2. Other than what has been described herein, to my knowledge, the United States has not attempted to obtain this data by other means.

///

///

///

VII. CONCLUSION

45. For all the reasons described above, there is probable cause to believe that RHAYEL violated 18 U.S.C. § 1957(a) (Transactional Money Laundering).

46. Further, there is probable cause to believe that the items listed in Attachment B, which constitute evidence, fruits, and instrumentalities of violations of the Subject Offenses will be found at the SUBJECT PREMISES, and on the persons of RHAYEL and GUAN as described in Attachments A-1 through A-3.

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone this 16th day of May 2023.

HONORABLE ALEXANDER F. MACKINNON
UNITED STATES MAGISTRATE JUDGE